Travaux pratiques – Visualiser les chapeaux noirs (version de l'instructeur)

**Remarque à l'intention de l'instructeur**: le texte en rouge ou surligné en gris apparaît uniquement dans la version de l'instructeur.

1. Objectifs

Rechercher et analyser les incidents liés à la cybersécurité

1. Contexte/scénario

En 2016, le coût annuel des cyberattaques pour les entreprises a été estimé à 400 millions de dollars. Les gouvernements, les entreprises et les particuliers sont de plus en plus ciblés par les cyberattaques et les incidents de cybersécurité se multiplient.

Au cours de ces travaux pratiques, vous allez créer trois profils de hacker hypothétiques, chacun composé d'une organisation associée, d'une attaque et d'une méthode permettant à l'entreprise de prévenir ou de neutraliser l'attaque.

**Remarque** : vous pouvez utiliser le navigateur sur la machine virtuelle installée lors d'un TP précédent pour lancer votre recherche sur les problèmes de sécurité. En utilisant la machine virtuelle, vous évitez d'infecter votre ordinateur avec des malwares.

1. Ressources requises

* Ordinateur personnel ou terminal mobile avec accès Internet

1. Qui est le hacker ?

**Hacker Anonyme :** Membre d'un groupe indépendant, souvent motivé par des idéaux, des revendications ou le simple désir de causer des perturbations. Ils peuvent utiliser des attaques telles que le déni de service distribué (DDoS) pour rendre des services indisponibles.

Plusieurs réponses sont possibles.

1. À quel groupe/organisation le hacker est-il associé ?

**Hacker Anonyme organisation associée :** Groupe de hackers indépendants.

Plusieurs réponses sont possibles.

1. Quel est le mobile du hacker ?

**Hacker Anonyme Mobile :** Perturbation, revendications idéologiques, plaisir du défi technique.

Plusieurs réponses sont possibles.

1. Quel type d'attaque a-t-il utilisé ?

**Hacker Anonyme Type d'Attaque :** Attaque par déni de service distribué (DDoS).

Plusieurs réponses sont possibles.

1. Quelles ont été la cible et la vulnérabilité utilisées pour atteindre l'entreprise ?

**Hacker Anonyme (Attaque DDoS) Cible :** Les infrastructures réseau de l'entreprise.

Plusieurs réponses sont possibles.

1. Comment cette attaque pourrait-elle être évitée ou neutralisée ?

**Hacker Anonyme (Attaque DDoS) :** Surveillance proactive du trafic réseau pour détecter les signes d'une attaque DDoS imminente et prendre des mesures pour atténuer l'impact, par exemple en redirigeant le trafic ou en activant des filtres.

Plusieurs réponses sont possibles.

1. Qui est le hacker ?

**Hacker Interne :** Un employé mécontent ou malveillant qui exploite sa position au sein de l'organisation pour voler des données sensibles. Les motivations peuvent inclure la vengeance, le gain personnel ou la collusion avec des tiers.

Plusieurs réponses sont possibles.

1. À quel groupe/organisation le hacker est-il associé ?

**Hacker Interne organisation associée :** Employé mécontent avec un accès privilégié.

Plusieurs réponses sont possibles.

1. Quel est le mobile du hacker ?

**Hacker Interne Mobile :** Vengeance, gain personnel, collusion.

Plusieurs réponses sont possibles.

1. Quel type d'attaque a-t-il utilisé ?

**Hacker Interne Type d'Attaque :** Vol de données sensibles.

Plusieurs réponses sont possibles.

1. Quelles ont été la cible et la vulnérabilité utilisées pour atteindre l'entreprise ?

**Hacker Interne (Vol de données) Cible :** Données sensibles de l'entreprise.

Plusieurs réponses sont possibles.

1. Comment cette attaque pourrait-elle être évitée ou neutralisée ?

**Hacker Interne (Vol de données) :** Détecter rapidement les comportements suspects à l'aide de systèmes de détection d'intrusion et d'analyse des journaux. Révoquer immédiatement les privilèges d'accès de l'employé concerné et mettre en œuvre des procédures de réponse aux incidents.

Plusieurs réponses sont possibles.

1. Qui est le hacker ?

**Hacker Étatique :** Un représentant d'une entité gouvernementale engagé dans des activités de cyber espionnage. Ces hackers sont souvent motivés par des objectifs géopolitiques, économiques ou stratégiques visant à obtenir un avantage compétitif.

Plusieurs réponses sont possibles.

1. À quel groupe/organisation le hacker est-il associé ?

**Hacker Étatique organisation associée :** Unité de cyber espionnage d'un État.

Plusieurs réponses sont possibles.

1. Quel est le mobile du hacker ?

**Hacker Étatique Mobile :** Espionnage industriel, avantages géopolitiques, stratégiques ou économiques.

Plusieurs réponses sont possibles.

1. Quel type d'attaque a-t-il utilisé ?

**Hacker Étatique Type d'Attaque :** Cyber espionnage, visant à infiltrer les réseaux pour collecter des informations confidentielles, stratégiques ou économiques au profit de leur gouvernement.

Plusieurs réponses sont possibles.

1. Quelles ont été la cible et la vulnérabilité utilisées pour atteindre l'entreprise ?

**Hacker Étatique (Cyber espionnage) Cible :** Informations stratégiques, économiques ou géopolitiques de l'entreprise.

Plusieurs réponses sont possibles.

1. Comment cette attaque pourrait-elle être évitée ou neutralisée ?

**Hacker Étatique (Cyber espionnage) :** Isoler les systèmes compromis, enquêter sur la portée de l'intrusion, et collaborer avec des agences gouvernementales ou organisations internationales pour partager des renseignements sur les menaces.

Plusieurs réponses sont possibles.